Encryption Technologies for End User Devices

Updated: July 28, 2009

I. Background

Various Montana state agencies have requested a guideline for properly securing sensitive data on laptop computers. In response to this request, the Encryption Group was formed by direction of the Information Technology Manager's Council (ITMC) board. The purpose of this document is to disclose the findings and recommendations of the Encryption Group.

During its initial research, the Encryption Group realized that the scope of the discussion needed to be expanded from laptop computer encryption to include other immediate threats of sensitive data on media such as desktop computer hard drives, USB flash drives, memory cards, external hard drives, and writeable disks. Therefore, the focus of this document is to identify several different types of encryption for stored data (data at rest), to discuss the best use for each type of encryption, and to offer scenarios and recommendations regarding practical working situations. This document does not address the encryption of transmitted data (data in motion).

II. Characteristics of Encryption Types

The following section is a condensed version of the National Institute of Standards and Technology Special Publication 800-111

A. Types of Encryption

The types of encryption that are available include:

Full Disk Encryption (FDE) is **t**he process of encrypting all the data on the hard drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product.

File Encryption is the process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided.

Folder Encryption is **t**he process of encrypting individual folders on a storage medium and permitting access to the encrypted files within the folders only after proper authentication is provided.

Virtual Disk Encryption is the process of encrypting a container, which can hold many files and folders, and permitting access to the data within the container only after proper authentication is provided.

Volume Encryption is the process of encrypting an entire volume and permitting access to the data on the volume only after proper authentication is provided.

B. A Table Showing the Different Characteristics of Storage Encryption Technologies:

Characteristic	Full Disk Encryption	Volume Encryption	Virtual Disk Encryption	File/Folder Encryption
Typical platforms supported	Desktop and laptop computers	Desktop and laptop computers, volume-based removable media (e.g., USB flash drives)	All types of end user devices	All types of end user devices
Data protected by encryption	All data on the media (data files, system files, residual data, and metadata)	All data in the volume (data files, system files, residual data, and metadata)	All data in the container (data files, residual data and metadata, but not system files)	Individual files/folders (data files only)
Mitigates threats involving loss or theft of devices?	Yes	Yes	Yes	Yes
Mitigates OS and application layer threats (such as malware and insider threats)?	No	If the data volume is being protected, it sometimes mitigates such threats.* If the data volume is not being protected, then there is no mitigation of these threats.	It sometimes mitigates such threats*	It sometimes mitigates such threats*
Potential impact to devices in case of solution failure	Loss of all data and device functionality	Loss of all data in volume; can cause loss of device functionality, depending on which volume is being protected	Loss of all data in container	Loss of all protected files/folders
Portability of encrypted information	Not portable	Not portable	Portable	Often portable

** These storage encryption technologies can only protect the files against some OS and application layer threats if the user has not been authenticated in this session to access the files. If a single sign-on solution is used, then generally the user is authenticated to the storage encryption technology during OS login, so the files are not protected against these threats once OS login occurs. If a separate authentication solution is used, the files are protected until that separate authentication is performed.*

SOURCE: National Institute of Standards and Technology (NIST) *"Guide To Storage Encryption Technologies for End User Devices"* p.3-7

C. Benefits

The following explains the types of protection each storage encryption technology can and cannot provide.

Full Disk Encryption. For a computer that is not booted, all the information encrypted by FDE is protected, assuming that pre-boot authentication is required. When the device is booted, then FDE provides no protection; once the OS is loaded, the OS becomes fully responsible for protecting the unencrypted information. The exception to this is when the device is in a hibernation mode; most FDE products can encrypt the hibernation file.

Virtual Disk and Volume Encryption. When virtual disk encryption is employed, the contents of containers are protected until the user is authenticated for the containers. If single sign-on is being used for authentication to the solution, this usually means that the containers are protected until the user logs onto the device. If single sign-on is not being used, then protection is typically provided until the user explicitly authenticates to a container. Virtual disk encryption does not provide any protection for data outside the container, including swap and hibernation files that could contain the contents of unencrypted files that were being held in memory. Volume encryption provides the same protection as virtual disk encryption, but for a volume instead of a container.

File/Folder Encryption. File/folder encryption protects the contents of encrypted files (including files in encrypted folders) until the user is authenticated for the files or folders. If single sign-on is being used, this usually means that the files are only protected until the user logs onto the device. If single sign-on is not being used, then protection is typically provided until the user explicitly authenticates to a file or folder. File/folder encryption does not provide any protection for data outside the protected files or folders, including swap and hibernation files that could contain the contents of unencrypted files that were being held in memory. File/folder encryption software also cannot protect the confidentiality of filenames and other file metadata, which itself could provide valuable information to attackers (for examples, files that are named by Social Security number).

D. Case Scenarios

(Each Enterprise Agency should come up with case scenarios that best fit their agency.)

Case 1: Traveling with a Laptop

A user occasionally travels on behalf of the organization and carries a laptop that contains sensitive data. For this data, the major threat that the organization needs to mitigate is unauthorized disclosure of data from the loss or theft of the laptop. Possible solutions include the following:

- Use the laptop's OS access control features to strictly limit where the user can save files. Implement volume, virtual disk, or file/folder encryption on the laptop to protect the user's files.
- Implement FDE on the laptop, and require pre-boot authentication.
- Provide the user with a loaner laptop when needed for travel. Protect the user's sensitive data on the laptop using either of the methods described above. When the user returns from travel, wipe and rebuild the loaner laptop to remove any traces of sensitive data from it. Using a loaner laptop in this way is particularly helpful if the laptop is being used in hostile environments, where the laptop is at greater risk of being compromised.

Case 2: Sharing a Laptop

Three users share a laptop. One of the users uses the laptop to access data that the other two users are not authorized to access. For this data, the major threats that the organization needs to mitigate are an insider threat from the other two users, and unauthorized disclosure of data from the loss or theft of the laptop. Possible solutions include the following:

- Implement volume, virtual disk, or file/folder encryption on the laptop. Protect the first user's data using the storage encryption software, with the authentication and cryptographic keys implemented so that only the first user, and not the other two users, can access the protected data. If there is concern about the first user always remembering where to save files, configure the laptop's access control so that the first user's data is all saved to a particular location, and protect that location with the storage encryption software.
- Store the data on external media, such as a flash drive or external hard drive, and use volume, virtual disk, or file/folder encryption to protect the media. The user needs to protect physical access to the media and to remember to save new or modified data to the media.
- Store the data on a remote system and give the first user access to the data through secured means (e.g., VPN). Provide the data in such a way that it is not saved to the laptop (e.g., the user views and modifies the remote data through a Web interface).

Case 3: Transferring Files Between Computers

A user edits documents using both a desktop PC at the organization's office and a personally owned computer at home. The user transfers documents between the computers on a daily basis using a USB flash drive. The two computers run different types of OSs. For the documents, the major threat that the organization needs to mitigate is unauthorized disclosure of data from loss or theft of the user's flash drive. Possible solutions include the following:

- Acquire and use a flash drive with self-contained storage encryption capabilities, such as encryption software and secure key storage.
- Acquire a volume, virtual disk, or file/folder encryption solution that will work on both PCs, and deploy it. Encrypt the documents using the solution and store the encrypted data on a flash drive.

Case 4: Sharing Data with Contractor

A user wants to provide a contractor with copies of large data sets on a daily basis because the contractor has no direct access to the system containing the data. The user will copy the data onto removable media for the contractor. For this data, the major threat that the organization needs to mitigate is unauthorized disclosure of data from loss or theft of the removable media. Possible solutions include the following:

- Deploy virtual disk or file/folder encryption software to the user and contractor's computers. Encrypt the data using the software and burn the encrypted data onto CDs or DVDs.
- Acquire USB flash drives or external hard drives that have built-in storage encryption capabilities. Store the copies of the data on the encrypted drives.
- Acquire USB flash drives or external hard drives. Deploy virtual disk, volume, or file/folder encryption software to the user and contractor's computers. Encrypt the data using the software and store it on the drives.

III. Advanced Encryption Standard (AES)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.
The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

IV. Recommendations

The working group recommends:

1. Adoption of Advanced Encryption Standard as the encryption standard for the State of Montana.

2. Deployments of encryption are managed centrally by agencies. Centralized management is most often performed through special management utilities provided by a storage encryption vendor. The capabilities of centralized management utilities for storage encryption technologies vary considerably. Examples of commonly implemented capabilities are as follows:

- Deploying storage encryption software to additional devices
- Updating storage encryption software (e.g., patching, upgrading)
- Configuring storage encryption software, such as specifying encryption algorithms and setting authentication policies (in some cases, the policies are specific for types of devices, groups of users, and/or individual users)
- Managing storage encryption authenticators and cryptographic keys
- Collecting and reviewing storage encryption-related logs
- Recovering stored information from device failures
- Performing routine system maintenance
- Enabling the encryption of data and managing encrypted storage

3. Agencies would also be well advised to not rely on storage encryption technologies to protect data without regularly maintaining the encryption solution. A new committee be formed to evaluate specific products. It would benefit the Enterprise to recommend a minimal number of solutions that would meet all agencies needs for encryption software. Benefits would include cost savings in purchasing the product, support, and research. The group recommends that the new committee work toward solutions that can be adopted as state standard(s).

IV. References and Additional Reading

A. Federal Information Processing Standards Publication 197

B. National Institute of Standards and Technology (NIST) Guide to Storage Encryption for End User Devices – Special Publication 800-111

C. Wikipedia – Comparison of disk encryption software
http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software

C. Other State Guides
Iowa
http://www.state.ia.us/itd/standards/documents/061219_Laptop.pdf
NewJersey
http://www.newjersey.gov/military/publications/dd/DD25-2-5.pdf
Norfolk State University
http://www.nsu.edu/oit/policies/OIT62.013AcceptableEncryptionPolicy.pdf
Commonwealth of Pennsylvania
http://www.portal.state.pa.us/portal/server.pt?open=512&objID=416&PageID=200500&mode=2&contentid=http://pubcontent.state.pa.us/publishedcontent/publish/cop_general_government_operations/oa/oa_portal/omd/p_and_p/itbs/domains/security/itbs/itb_sec020.html